26 JUL 1978

MEMORANDUM FOR: D/OCR

SUBJECT: Implementation of Classification Guidelines

1. This office will primarily work with derivative information and will retain originators classifications and controls.

2. The following "oddball" areas which require protection are specific to this office but some also may pertain to other offices. STAT

[redacted]

C. Some computer programs are of themselves, i.e. without a data base, classified because the program itself can provide the methodology used in doing sensitive studies.

D. The question of "confidentiality" in dealing with contractors doing unclassified studies needs to be addressed.

E. Guidance--a warning, if you will--that basic research prohibited from classification when used alone may very well become classified when, for example, judgmental

SUBJECT: Implementation of Classification Guidelines

statements about its applicability to a weapon system are interwoven with it. Some net assessments may fall into this category. STAT

[redacted]

4. For classified correspondence, again a code that could be preprinted or stamped on the face when a document is to be classified more than 6 years. Such a code would be like the use of E2 IMPDET and would refer back to previously set criteria. For example, the classifier might be 007 and Y-6 might be used to indicate that this is SCI material and therefore will retain classification 20 years.

5. Some way of indicating foreign information would be useful. The use of one foreign information document in finished intelligence with scores of other sources should not make the finished intelligence classified for 30 years.

6. I would like to see as general guidelines in any guide the classification criteria specified in the early April draft of 11652 (attached). They are most useful in thinking of national security.

STAT [redacted]

Chief
Intelligence Production Staff/SI

Attachment:
Draft Section of 11652

expected to cause outweighs the public interest in access to the information. The unauthorized disclosure of foreign government information or the identity of a foreign source is presumed to cause at least significant damage to the national security.

(d) Classification Criteria. Information may not be considered for classification unless its disclosure reasonably could be expected to:

(1) Make the United States or its allies vulnerable to attack by a foreign power, or weaken the ability of the United States or its allies to conduct armed operations or defend themselves, or diminish the military or operational effectiveness of the United States' armed forces; or

(2) Lead to hostile political, economic, or military action against the United States or its allies by a foreign power; or

(3) Reveal, in whole or in part, the defense or foreign policy plans or posture of the United States or its allies; provide a foreign nation with information upon which to develop effective countermeasures to such plans or posture; weaken or nullify the effectiveness of a United States military, foreign policy, foreign intelligence, or foreign counterintelligence plan, operation, project, or activity of significance to the national security; or

(4) Aid a foreign nation to develop or improve its military capability; or

(5) Reveal, jeopardize, or reduce the effectiveness of an intelligence or cryptologic source, method, device, or system; or

(6) Disclose to other nations or foreign groups that the United States has, or is capable of obtaining, certain information concerning those nations or groups without their knowledge or consent; or

(7) Deprive the United States of a diplomatic, military, scientific, engineering, technical, economic, or intelligence advantage related to the national security; or

(8) Create or increase international tensions; cause or contribute to political or economic instability or civil disorder in a foreign country; or otherwise significantly impair the foreign relations of the United States; or

(9) Disclose or impair the position of the United States or its allies in international negotiations; or

(10) Disclose the identity of a confidential foreign source; or

(11) Disclose foreign government information; or

(12) Diminish significantly the effectiveness of United States Government programs for safeguarding nuclear materials or facilities; or

(13) Place a person's life in jeopardy.

(e) Limitation on Duration of Classification.

(1) Each original classification authority shall, at the time of original classification, set a date or event for automatic declassification or for review to decide whether the information can be declassified as early as national security considerations will permit. Except as permitted in paragraph (2) below, the information shall be declassified no more than six years from the date of original classification.

(2) Only officials with Top Secret classification authority and heads of agencies listed in Section 2(b) may classify information for more than six years from the date of original classification. In such cases, the date or event for declassification or review shall be as early as national security permits and shall be no more than twenty years after the original classification, except that the date or event for declassification or review of foreign government information may be up to thirty years. This authority shall be used sparingly, and in each case of its use the justification for the longer period shall be recorded on the document. This justification may be by reference to criteria set forth in agency implementing directives.

(f) Classification Identification and Marking.

(1) The following shall be shown on the face of the document at the time of its original classification: (i) the identity of the original classification authority; (ii) the office of origin; (iii) the date of the document's origin; (iv) the date or event for declassification or review; and (v) one of the three classification designations defined herein. When the individual who signs or otherwise authenticates a document or item also is authorized to classify it, no further annotation as to his identity is required. Documents classified for more

RECORDS AND CORRESPONDENCE

HN [redacted]
28 July 1978

STAT

EXECUTIVE ORDER 12065
NATIONAL SECURITY INFORMATION

On 28 June 1978 the President signed Executive Order 12065 concerning classification, declassification, and safeguarding of national security information. It replaces Executive Order 11652 and becomes effective on 1 December 1978. An Agency task force has been established under the Deputy Director for Administration to develop internal policies and procedures for implementing the new Order. As these policies and procedures are developed and approved, they will be made available to Agency employees. In the meantime it is recommended that all employees whose duties will be affected by the new Executive Order make every effort to become as familiar as possible with its requirements.

JOHN F. BLAKE
Deputy Director
for
Administration

DISTRIBUTION: ALL EMPLOYEES

25 July 1978
DRAFT

Coordination Staff Contribution To:
CIA Implementing Regulation to E.O. 12065

1. "Foreign government information", i.e., information that is passed to the agency by foreign governments, must be protected in the following manner:

a. Stamp the NOFORN caveat on all classified intelligence documents received from foreign governments -- in order to observe the so-called "third-country" rule. This would apply to all reports received in liaison channels from the four Commonwealth countries, the Germans, and other foreign liaison services.

b. Add a stamp on such documents received from foreign governments that they are exempt from automatic declassification and twenty year systematic review as specified in #3-404 of E.O. 12065.

2. Finished intelligence incorporating information provided by foreign governments will be exempt from automatic declassification and systematic review after twenty years as required by Section 3, Paragraph

404 of E.O. 12065. In order to establish that this exemption applies to particular finished intelligence some identification is necessary. This might be done simply by adding "3C" for Third Country to "NOFORN," Thus: "NOFORN 3C." Alternatively, a new control caveat could be authorized, such as "FORCON" for "Foreign Originator Control," to indicate that a foreign government must be consulted before a finished intelligence item is declassified or downgraded.

3. Section 3, Paragraph 404 states that agency heads may consult "where appropriate" with foreign governments on declassification matters. The agency receives sensitive intelligence information from certain close allies under the express agreement that it will not be reclassified without permission of the government releasing the information. Should the United States Government be perceived by intelligence services of foreign governments to be making unilateral decisions on the declassification of third-country intelligence information, the chances that cooperating services would then withhold information would be significantly increased. It is therefore always appropriate to consult with the foreign government or international organization concerned, as long as the

governing authority or the international organization that provided the information continues to exist. Where the government or international organization ceases to exist, as, for example, in the case of pre-Communist Czechoslovakia, South Vietnam, or the League of Nations, the obligation to protect third-country or third-party sourcing and information ceases, and such consultation is not possible.

25X1

Chief, NFAC Coordination Staff